

SSRO-C-124: Outsourced Services

Appendix 3: Service Specification - HR

* + 1. This Specification of service covers the requirements to deliver an Outsourced HR Solution.
		2. Provision of HR services must maintain a fully managed integrated service which provides for HR administration functions including self-service functionality.
		3. The SSRO has three different level of users:
			- Administrator who will have full system access, and be able to create and run reports;
			- Line Manager who will be able to review limited information on their direct reports (holiday, salary information, bonuses, training records and sickness) and be able to approve self-service requests (ideally the system will have the facility to delegate this responsibility on a temporary basis); and
			- Self-service users who will be able to see and update their own personal, salary, sickness, holiday, and training details via self-service access.
		4. HR Service includes, but is not limited to the following key deliverables via an electronic, web-based system:

Key deliverables:

* + - * Employees Personal Information to;
			* Employment Details;
			* Absence Recording;
			* HR Management Information Reporting;
			* Employee Self Service;
			* Training; and
			* Administration of New Starters and Leavers.
			* An annual appraisal system

Additional Deliverable:

* + - * Organisational Structure
		1. The H R System must hold Employee Personal Information for each SSRO employee, including:
			- Personal details (full name, preferred name, gender, and date of birth);
			- Address details;
			- Contact details;
			- Emergency contacts and next of kin;
			- Driving licenses;
			- Private vehicles;
			- Passports; and
			- Sensitive information such as equality data.
			- Security clearance details
		2. The HR System must hold Employment Details for each SSRO employee, including:
			- Salary;
			- Benefits (such as pensions, bike loans and season tickets);
			- Hours and basis;
			- Terms and conditions;
			- Employment history;
			- Working patterns;
			- Reporting hierarchy;
			- Reckonable service; and
			- Leaver information.

Additional Deliverable:

* + - * Person photograph.
		1. The HR System must record holiday and sickness absence with the personal holiday scheme linked to the Employee Self-Service system (Absence Recording).
		2. The HR System must deliver standardised reporting (HR Management Information Reporting) and allow for the SSRO to run reports with its own defined parameters. These reports should be able to be downloaded unto CSV format or excel as follows:
			- People reports;
			- Absence reports;
			- Structure reports;
			- Payroll reports; and
			- Training.

Additional Deliverable:

* + - * Adaptable search feature with reporting facility.
			* Facility to set and adapt reports
		1. The HR System must provide cloud-based employee self-service (Employee Self-Service). Self-service to include:
			- Updating personal details;
			- Booking holidays and sickness with management approval work flows; and
			- Recording and training events
			- And to support the annual appraisal system.

Additional Deliverables:

* + - * Booking training events
			* The HR System to reflect the SSRO's organisational structure. The organisational structure may be updated periodically by the SSRO.
1. IT and Security
	* 1. In carrying out its corporate functions, the SSRO processes information of the following kinds:
			+ **Official information**, which may be marked **OFFICIAL SENSITIVE** with the Government Security Classifications.
			+ **Confidential or commercially sensitive information**, which the SSRO would not disclose under the Freedom of Information Act 2000 by reason of the application of one of the exemptions in that Act.
			+ **Personal data or special category data** within the meaning of the UK General Data Protection Regulation and the Data Protection Act 2018 which must be processed in accordance with applicable data protection law.
		2. The SSRO takes the security of the information it holds seriously, and the Supplier shall comply with the Security Measures and Security Requirements contained in the contract, including those related to OFFICIAL-SENSITIVE information.
		3. The SSRO’s IT environment, policies and procedures are based on the following policies and procedures and the system(s) provided by the Supplier for SSRO staff use must operate in this environment:
			+ HMG Security Policy Framework (SPF).
			+ NCSC Published Guidance, Cloud Security Principles and Security Design Principles.
			+ ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.
			+ ISO/IEC 22301:2012 – Societal Security – Business Continuity Management Systems – Requirements.
			+ Cyber Essentials Scheme: Requirement for Technical Protection from Cyber Attacks.
		4. Any accreditations the Supplier confirms it holds, or intends to hold at the Commencement Date, shall be maintained throughout the Contract Period. Such accreditations may include:
			+ ISO22301:2012 Business Continuity Management certification;
			+ ISO20000 IT Service Management certifications; and
			+ ISO27001:2013 certification (to the extent it is not already a requirement for the Supplier to hold it pursuant to paragraph 5.6 below).
		5. The SSRO maintains Cyber Essentials Plus certification and the Supplier shall have and maintain Cyber Essentials Plus (or equivalent) accreditation for the Contract Period.
		6. The Supplier (or, in the event the Supplier sub-contracts all or part of the provision of the IT system, that sub-contractor) must hold Cyber Essentials Plus (or equivalent) and ISO27001:2013 (or equivalent) accreditation for the Contract Period.
		7. The SSRO maintains the Cyber Essentials Plus certification. All systems provided for the SSRO’s use must meet the Cyber Essentials and Cyber Essentials Plus requirements.
		8. The SSRO’s IT environment uses the Microsoft platform including Windows 10, Office 365, Intune and Enterprise Mobility and Security. This is complemented by infrastructure services including Azure virtualisation, Cisco Switches and ASA firewalls, and wireless networking using Cisco Meraki access points. Staff work regularly and frequently away from the office. Secure connectivity, within the office and when working remotely, is provided through a Zero Trust Architecture solution that utilises iBoss (https://www.iboss.com/). The Supplier must ensure that full system functionality is available to different SSRO user groups when connected to the office network and when working remotely. The SSRO’s Secure Operations Centre (SOC) is currently provided by e2e assure (see [**https://www.e2e-assure.com/SCC**](https://www.e2e-assure.com/SCC)).
		9. The Supplier must notify the SSRO of the physical locations where data (including personal data) may be stored, processed, or managed by the Supplier and any third-party cloud platform provider. The Supplier shall not transfer any data (including personal data) outside of the UK unless the prior written consent of the SSRO has been obtained, which will be subject to conditions as provided in the Contract. If provision of the Services includes offshoring of data outside the UK, the Supplier must ensure that any necessary additional security provisions required by the SSRO (such as obfuscating IPR related or commercially sensitive data) are in place and that the prior written consent of the SSRO has been obtained.
		10. A single sign on solution is desirable, and, in case this cannot be provided by the Supplier in the context of the SSRO environment specified above, multi factor authentication for all users must be implemented, managed, and maintained by the Supplier.
2. Training and Ongoing Support
	* 1. The Supplier shall train up to 5 staff from the SSRO on the functionalities and use of their technology/software platform, no later than the Service Commencement Date.
		2. The Supplier shall provide ongoing training as reasonably required to ensure a smooth running of the service and to foster greater understanding and ensure service delivery.
		3. The Supplier shall provide facilities and or use remote access solutions as required, Training Materials and suitable qualified resources for the training.
3. Set up and transition
	* 1. The Implementation Period shall commence upon contract award – currently estimated to be 1 February 2024. The Supplier will be required to plan the transition and undertake any necessary transition activities in time for the new operational payroll service to run from 1 July 2024.
		2. The Supplier must manage the effective migration of all current year and historical data (2 year’s data) from the SSRO’s existing Supplier. This must be supported by an audit trail that will be subject to SSRO and audit review.
		3. The Supplier shall work with the incumbent Supplier and the SSRO during the Implementation Period to ensure that, at the Service Commence Date, the Implementation is completed, and the Services are provided fully in accordance with the Specification and the Supplier’s Response.
		4. The Supplier shall deploy (including installation, where applicable) the technology solution in preparation for data transfer in accordance with IT Security conditions.
		5. Implementation is deemed to have been completed/ accepted (and payments in respect of the Services carried out during the Implementation Period, where relevant, will fall due) when:
			+ The functionalities are tested and operable;
			+ The system meets with SSRO security requirements;
			+ Training of SSRO Staff is completed; and
			+ SSRO has access to the system from its designated offices as well as owner VPN (outside the office).
		6. There may be a need for parallel running of the service, during the implementation period and to ensure data accuracy.

**Annex 2 – Performance Standards and Key Performance Indicators**

1. **System maintenance**
	1. The Supplier will ensure that the System/software(s) is maintained in line with the manufacturer’s instructions, which must include any quality assurance checks and service programme maintenance schedules as agreed and set out in the contract.
	2. Planned servicing will take place at a frequency pre-agreed by the Parties to this contract, or more frequently if deemed necessary by the Supplier, at no additional cost to SSRO.
2. **Uptime guarantee**
	1. The Supplier system(s) will achieve 98% availability rate for full use by the SSRO at its site and remotely (“Uptime”)
	2. Uptime shall be measured on a 12 hours day (9am to 9pm, Monday to Friday, except weekends and UK Bank Holidays), 5 days a week basis over fixed three-month periods beginning on the Service Commencement Date (herein a “Quarterly Period”) – see table below.

|  |  |
| --- | --- |
| **Service Support and Uptime** | **KPI Target Requirement** |
| Uptime Guarantee | 98% |
| First time fix (within 4 hours) | 98% |
| Service Response Time  | **Priority** within 3 working hours**Non-Priority** within 6 working hours |
| Telephone Support | Within 30 minutes of original call |

* 1. Supplier system will be considered unavailable if:
	+ unable to properly perform its core functions because of a network malfunction;
	+ system/software is not producing correct results; and/or
	+ the software provided by the Supplier which supports the service are not fully operational to a level which would support full proper use by the SSRO for any reason, providing it is the fault of the Supplier.

**3 Performance Indicators and Reports**

3.1 The table below sets out the Key Performance Indicators which the Contactor will measure to support the performance of the Outsourced Finance Support Services.

**Key Performance Indicators**

|  |  |
| --- | --- |
| **HR Service**  | **Requirement**  |
| Monthly reporting, to be agreed, but expected to be:  * No of employees/ structure
* Absence
* Payroll
* Holiday booked and outstanding
* Training booked
* Diversity reports
 | By 2nd working day each month   |
| Communication of planned downtime  | 5 working days   |
| Initial communication of any other downtime  | Within 2 hours   |
| **Service Support and Uptime**  | **Requirement**  |
| Uptime Guarantee  | 98%  |
| First time fix  | 98%  |
| Service Response/Resolution Time   | Priority within 3 working hours  Non-Priority within 6 working hours  |
| Telephone Support  | Within 30 minutes of original call  |

3.2 The Supplier shall monitor its performance against each Performance Indicator and send the Authority a report on a quarterly basis (Service Period) detailing the level of performance achieved in accordance with Performance monitoring report.

3.3 The Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information:

* Information in respect of the Service Period just ended for each Key Performance Indicator;
* the actual performance achieved over the Service Period, and that achieved over the previous 3 Service Periods;
* a summary of all Performance Failures that occurred during the Service Period;
* which Performance Failures remain outstanding and progress in resolving them;
* for any KPI Failures occurring during the Service Period, the cause of the relevant KPI Failure and the action being taken to reduce the likelihood of recurrence;
* the status of any outstanding Rectification Plan processes, including:
* relevant particulars of any aspects of the Supplier’s performance which fail to meet the requirements of this Agreement;
* such other details as the SSRO may reasonably require from time to time.